

**DETAILED ACTION**

***Response to Arguments***

In view of the appeal brief filed on **07/18/2011**, PROSECUTION IS HEREBY REOPENED. As set forth below;

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,  
(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

**EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with **Mr. James A. LaBarre** on 10/06/2011.

The application has been amended as follows:

1. (Cancelled).
2. (Cancelled)
3. (Cancelled).
4. (Previously Presented) The handset according to claim 18, wherein the secure electronic module is a UICC.
5. (Previously Presented) The handset according to claim 18, wherein the operating system controls the authentication of the secure electronic module by the storage support module.
6. (Cancelled)

7. (Previously Presented) The handset according to claim 18, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

8. (Cancelled).

9. (Cancelled).

10. (Currently Amended) The method of claim 9 19, wherein the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. (Previously Presented) The method of claim 19, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

12. (Previously Presented) The handset according to claim 4, wherein the operating system controls the authentication of the secure electronic module by the storage support module.

13. (Previously Presented) The handset according to claim 4, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

14. (Previously Presented) The handset according to claim 5, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

15. (Currently Amended) The handset according to claim 6 18, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

16. (Currently Amended) The method of claim 9 19, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

17. (Previously Presented) The method of claim 10, wherein the s secure electronic module blocks the use of the handset when a false IMEI is detected.

18. (Currently Amended) A telephone handset, comprising:  
a storage support module storing an International Mobile Equipment Identity (IMEI) associated with an operator of a communication network;  
a secure electronic module;  
a processor;  
a memory device including program instructions that, when executed by the processor, control the handset to:  
authenticate, by the secure electronic module, the storage support module;

establish, in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module by means of encryption keys stored in the secure electronic module and the storage support module that are used to encrypt the secure communication channel;

transmit, via the secure communication channel, the IMEI from the storage support module to the secure electronic module;

transmit the IMEI to a mobile telephone operator by means of a secure OTA channel; and

enable, by the secure electronic module, the handset to access the communication network.

19. (Currently Amended) A method of securing a telephone handset, said method comprising:

authenticating a storage support module by a secure electronic module, said storage support module storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;

establishing, by a processor in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module by means of encryption keys stored in the secure electronic module and the storage support module that are used to encrypt the secure communication channel;

transmitting, via the secure communication channel, the IMEI from the storage support module to the secure electronic module;

transmitting the IMEI to a mobile telephone operator by means of a secure OTA channel; and

enabling, by the secure electronic module, the handset to access the communication network using the IMEI.

20. (Currently Amended) A telephone handset, comprising:  
a storage support module storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;  
a secure electronic module;  
means for authenticating the storage support module by the secure electronic module;

means for establishing, in the event the means for authenticating determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module by means of encryption keys stored in the secure electronic module and the storage support module that are used to encrypt the secure communication channel;

means for transmitting, via the secure communication channel, the IMEI from the storage support module to the secure electronic module;

means for transmitting the IMEI to a mobile telephone operator by means of a secure OTA channel; and

means for enabling the handset to access the communication network using the IMEI.

***Allowable Subject Matter***

1. Claims 4, 5, 7, and 10-20, are allowed.

2. The following is an examiner's statement of reasons for allowance:

According to the Applicant's arguments in the Pre-Appeal Brief mailed 07/18/2011, and the authorized Examiner's amendments. The prior art references (Simmons and Portalier) does not disclose "A telephone handset, comprising: a storage support module storing an International Mobile Equipment Identity (IMEI) associated with an operator of a communication network; a secure electronic module; a processor; a memory device including program instructions that, when executed by the processor, control the handset to: authenticate, by the secure electronic module, the storage support module; establish, in the event the secure electronic module determines that the storage support module is authentic, **a secure communication channel between the storage support module and the secure electronic module by means of encryption keys stored in the secure electronic module and the storage support module that are used to encrypt the secure communication channel;** transmit, via the secure communication channel, the IMEI from the storage support module to the secure electronic module; **transmit the IMEI to a mobile telephone operator by**

**means of a secure OTA channel;** and enable, by the secure electronic module, the handset to access the communication network."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OMONIYI OBAYANJU whose telephone number is (571)270-5885. The examiner can normally be reached on Mon - Fri, 7:30 - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KAMRAN AFSHAR can be reached on 571-272-7796. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/O. O./  
Examiner, Art Unit 2617

/KAMRAN AFSHAR/  
Supervisory Patent Examiner, Art Unit 2617